



U.S. Department of Justice

Criminal Division

Assistant Attorney General

Washington, D.C. 20530

January 26, 2011

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Room TW-A325
Washington, DC 20554

Dear Ms. Dortch:

On December 22, 2010, the President signed Public Law No. 111-331, the Truth in Caller ID Act of 2009, which prohibits the use of false caller ID information for the purpose of committing fraud or causing harm. This letter expresses the views of the United States Department of Justice regarding the public safety and law enforcement concerns that the Federal Communications Commission should address in the implementing regulations that the Act directs the Commission to adopt. We believe that the Commission can act to protect public safety and to promote the effective and efficient enforcement of our Nation's laws by adopting regulations that encourage the responsible provision of caller ID spoofing services.

I. Background

The Truth in Caller ID Act addresses caller ID spoofing, i.e., altering the telephone number displayed to the recipient of a telephone call to a number different than the caller's actual telephone number.¹ Although caller ID spoofing once required special equipment and/or a relatively high degree of technical sophistication, there are now widely available services that make caller ID spoofing as simple and inexpensive as placing a call with a traditional telephone calling card.

The widespread availability of caller ID spoofing services is a significant facilitator of criminal activity and a substantial threat to public safety. Numerous examples from around the country demonstrate these concerns, including the incidents described below:

¹ The notion of spoofing does not include caller ID *blocking* – i.e., preventing any caller ID from being displayed, a capability that telecommunications carriers generally are required to support. *See* 47 C.F.R. § 64.1601(b). Nor should spoofing be understood to include transmitting a number related to a private branch exchange (PBX) or the main telephone number of a business's network in place of an extension.

- Spoofed caller ID services have enabled a particularly insidious form of fraud known as “swatting.” Swatting refers to the practice of placing false emergency calls to law enforcement for the purpose of eliciting a response from the Special Weapons and Tactics (“SWAT”) team, usually as a means of revenge. In one of the largest swatting cases to date, Stuart Rosoff and a number of co-conspirators pled guilty to participating in a swatting conspiracy that targeted more than 100 victims. Using a spoofing service, Rosoff and his co-conspirators were able to place calls to the police that appeared to originate from the home telephone of their chosen victim. In these calls, one of the conspirators would identify himself to police as a member of the targeted family. The imposter would then tell police that he had shot and killed several members of the family and was holding the remaining family members hostage. Believing the emergency to be real, law enforcement would respond on an emergency basis, leading to dangerous confrontations between heavily armed police officers and the innocent victims of the “swatting” incident. At least two injuries resulted.
- Caller ID spoofing services are often used in connection with stalking and harassment. For example, in 2008, Danielle Zimmer and Carmen Veneziale pled guilty to harassment and making terrorist threats. Zimmer and Veneziale used a spoofing service to place 13 different calls to the cell phones of Zimmer’s co-workers. The calls were placed in the middle of the night and, as a result of a spoofing service, appeared to originate from the victim’s home telephone number. During the calls, Veneziale would inform the victims that he had broken into their home and was watching them.
- Caller ID spoofing services are also widely used by identity thieves. In one long-running scam, members of the public are called from a spoofed telephone number associated with the local court. Call recipients are told they missed their scheduled jury duty and are threatened with prosecution. The victims are then ordered to provide personally identifying information, including their Social Security number.
- Identity thieves also use caller ID spoofing services to access cellular telephone voicemail. When a call appears to originate from a user’s cellular telephone, most cellular providers do not require a password in order to access the user’s voicemail account. As a result, identity thieves are able to access most cellular telephone voicemail systems simply by spoofing the victim’s cellular telephone number. According to news reports, more than 50 voicemail accounts – including several belonging to celebrities – were accessed in this manner in a 2006 incident.

Widespread availability of caller ID spoofing services also enables criminals to more effectively hide their activities from law enforcement and significantly complicates evidence collection by law enforcement.

II. Recommendations

1. Rules Governing Providers of Caller ID Spoofing Services

Chairman Richard Boucher, whose subcommittee reported the House companion bill, introduced the bill on the House floor. At that time, he elaborated on the rules that Congress expects the FCC to adopt pursuant to the legislation:

In the rulemaking that the FCC will conduct pursuant to new subsection 227(e)(3) of the Communications Act, the committee anticipates that the commission will consider imposing obligations on entities that provide caller ID spoofing services to the public. The widespread availability of caller ID spoofing services presents a significant potential for abuse and hinders law enforcement's ability to investigate crime.

The prohibition in this bill on the use of those services with the intent to defraud, cause harm, or wrongfully obtain anything of value could be of limited value if entities continue to provide those services without making any effort to verify their users' ownership of the phone number that is being substituted.²

Chairman Boucher's floor statement upon passage of the Act also reflects the expectations of the full House Energy and Commerce Committee, which included a nearly identical statement in its report on the companion bill, H.R. 1258.³

As Representative Boucher explained, in order to fulfill the purpose of the Truth in Caller ID Act, it is necessary to ensure that caller ID spoofing services are not havens for criminal activity. Although outlawing the use of caller ID spoofing services for criminal purposes is a good first step, it is unlikely that criminals who are already intent on breaking the law are going to be significantly deterred from spoofing caller ID by the potential for an additional criminal charge. By directing the Commission to adopt rules to implement the Act, Congress expressed its intent that the Commission adopt such regulations as it finds necessary and feasible to address the problems caused by the widespread public availability of caller ID spoofing services.

The Department of Justice shares Congress' concern about the ready availability of services that allow users to spoof telephone numbers with which they have no association

² 156 Cong. Rec. H8378 (daily ed. Dec. 15, 2010) (statement of Rep. Boucher), available at http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?position=all&page=H8378&dbname=2010_record.

³ See House Comm. on Energy and Commerce, Truth in Caller ID Act of 2010, H.R. Rep. No. 461, 111th Cong., 2d Sess. 8 (2010), available at <http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr461&dbname=111&>.

whatsoever. Accordingly, the Commission should consider the feasibility of requiring public providers of caller ID spoofing services to make a good-faith effort to verify that a user has the authority to use the substituted number, such as by placing a one-time verification call to that number. In addition, the Commission should consider technical standards that would permit call recipients to determine whether caller ID information has been altered, and allow law enforcement to trace such calls to the true originating telephone number with appropriate authority.

2. The Law Enforcement and Court Orders Exceptions

Section 2 of the Act provides that “lawfully authorized investigative, protective, or intelligence activity” of a law enforcement or intelligence agency are not to be affected by the prohibitions within the Act. To ensure that lawful investigations are not impeded, the Act also specifically directs the Commission to include in its regulations an exemption for law enforcement agencies and court orders. *See* § 227(e)(3)(B)(ii)(I), (II).

The exemption for law enforcement agencies can be modeled on many existing statutory exemptions for the same purposes, including sections 1028 and 1030 of Title 18 of the United States Code. The Department recommends the following language:

- (a) This subsection does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.*
- (b) This subsection does not prohibit any activity in connection with a court order that specifically authorizes the use of caller identification manipulation.*

3. The Definition of “IP-Enabled Voice Service”

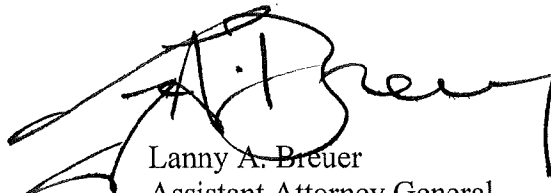
Finally, the Act defines the offense using the phrase “in connection with any telecommunications service or IP-enabled voice service.” *See* § 227(e)(1). The Act provides that the term “IP-enabled voice service has the meaning given that term by section 9.3 of the Commission’s regulations (47 C.F.R. 9.3), as those regulations may be amended by the Commission from time to time.” § 227(e)(8)(C). Given that section 9.3 does not currently define that term, the Commission should adopt a definition consistent with the public interest and with the purpose of the legislation. Such a definition could be modeled on the one already existing in 18 U.S.C. § 1039(h)(4):

IP-enabled voice service. - The term “IP-enabled voice service” means the provision of real-time voice communications offered to the public, or such class of users as to be effectively available to

the public, transmitted through customer premises equipment using TCP/IP protocol, or a successor protocol, (whether part of a bundle of services or separately) with interconnection capability such that the service can originate traffic to, or terminate traffic from, the public switched telephone network, or a successor network.⁴

The Department looks forward to working with the Commission on its adoption of rules as required by the Truth in Caller ID Act.

Respectfully submitted,



Lanny A. Breuer
Assistant Attorney General

⁴ 18 U.S.C. § 1039(h)(4) (defining the term for purposes of implementing the Telephone Records and Privacy Protection Act of 2006, which protects confidential phone records information).